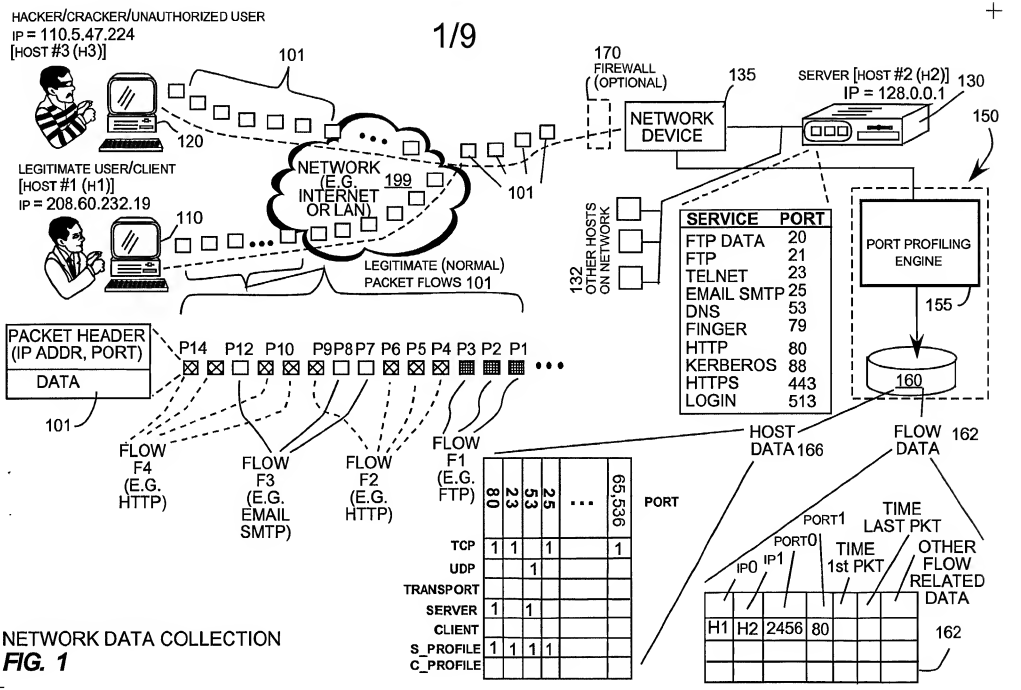
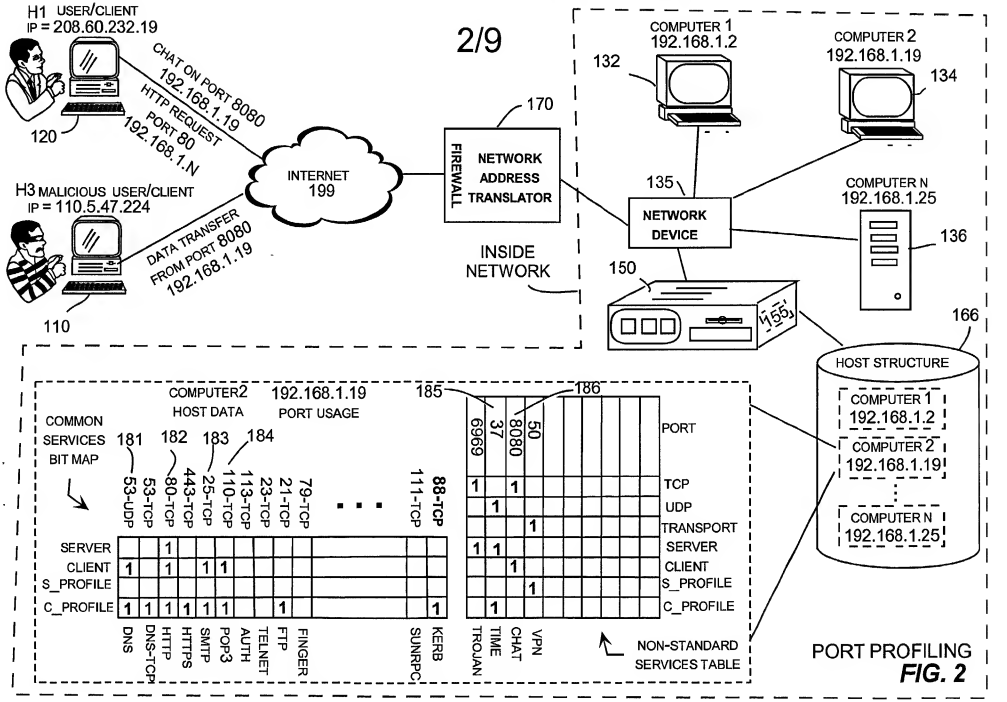
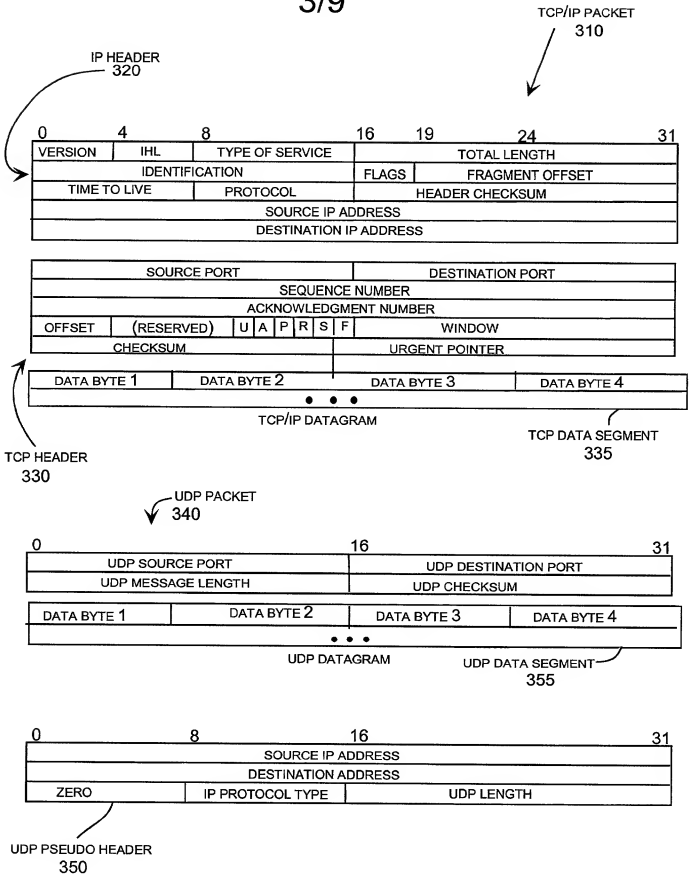


NETWORK DATA COLLECTION

FIG. 1



PORT PROFILING
FIG. 2



PACKET HEADERS

FIG. 3

TCP/IP SESSION
400

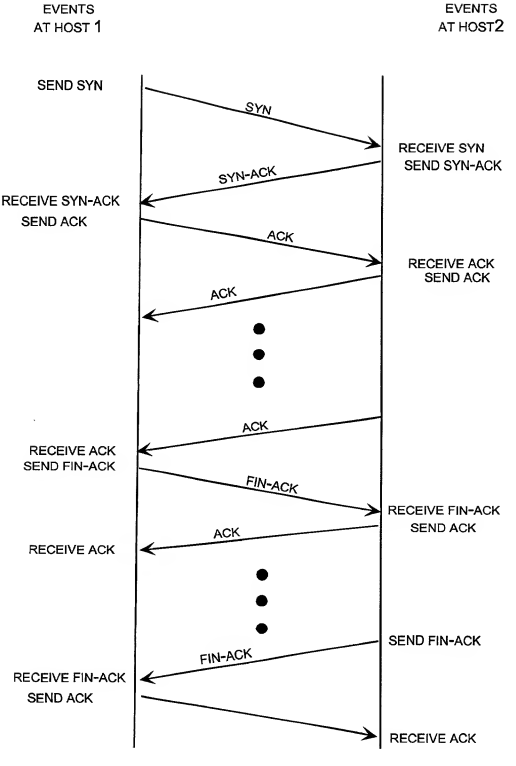


FIG. 4

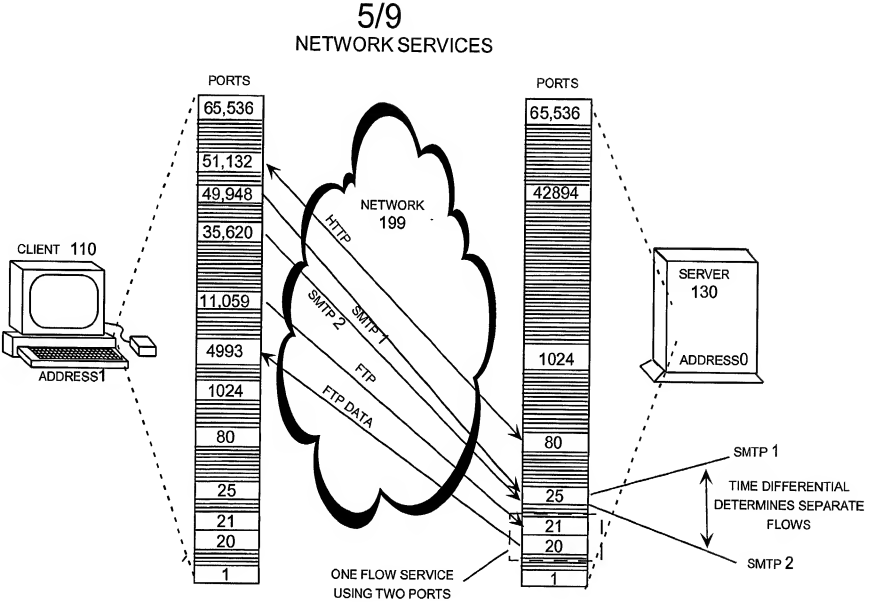

NETWORK SERVICES
PORTS
65,536
51,132
49,948
35,620
11,059
4993
1024
80
25
21
20
1
CLIENT 110
ADDRESS1
NETWORK
199
HTTP
SMTP 2
SMTP 1
FTP
FTP DATA
PORTS
65,536
42894
1024
80
25
21
20
1
SERVER
130
ADDRESS0
SMTP 1
TIME DIFFERENTIAL
DETERMINES SEPARATE
FLOWS
SMTP 2
ONE FLOW SERVICE
USING TWO PORTS

FIG. 5

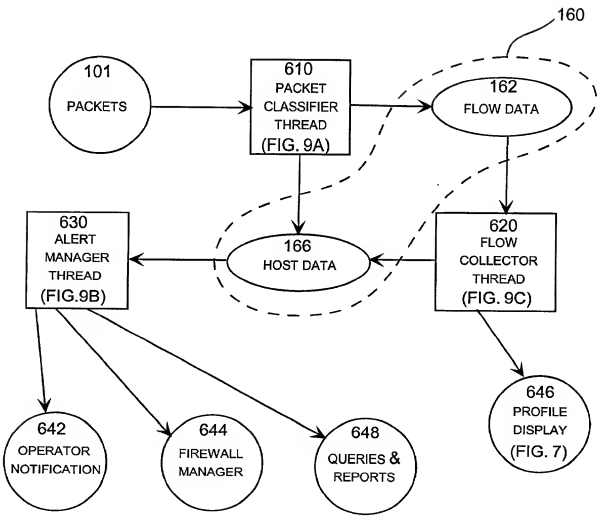

PORT PROFILING ENGINE
155
160
101
PACKETS
610
PACKET
CLASSIFIER
THREAD
(FIG. 9A)
162
FLOW DATA
630
ALERT
MANAGER
THREAD
(FIG.9B)
166
HOST DATA
620
FLOW
COLLECTOR
THREAD
(FIG. 9C)
642
OPERATOR
NOTIFICATION
644
FIREWALL
MANAGER
648
QUERIES &
REPORTS
646
PROFILE
DISPLAY
(FIG. 7)
PROGRAM THREADS: SQUARES
DATA STRUCTURES: OVALS
DATA INPUT/OUTPUT: CIRCLES

FIG. 6

Patent Application

PROFILE DISPLAY
700

SERVICE PROFILE

710 SERVERS

STANDARD OR COMMON SERVICES 730

735

	HOST IP	DNS	DNS TCP	HTTP	HTTPS	SMTP	POP	SNMP	TEL-NET	FTP	SSH	AFP IP	NET-BIOS	FNGR	NEWS	M'CAST	B'CAST	NON STANDARD SERVICES
721	066.056.047.148				◆						◆	◈				◆		◈P-2
722	066.056.065.002																◆	◆U-67
723	066.056.065.003																◆	
724	066.056.065.006	◆																
725	066.056.079.001																	
726	066.056.169.191																	

741

750 CLIENTS

760 STANDARD OR COMMON SERVICES

773

755

	HOST IP	DNS	DNS TCP	HTTP	HTTPS	SMTP	POP	SNMP	TEL-NET	FTP	SSH	AFP IP	NET-BIOS	FNGR	NEWS	M'CAST	B'CAST	NON STANDARD SERVICES
761	066.056.047.148	◆		◆	◈	◈	◆			◈	◈	◈						◆U-67 ◈T-43
762	066.056.065.002																	
763	066.056.065.003																	
764	066.056.065.006																	
765	066.056.079.001				◇													
766	066.056.169.191																	

777

◆ IN PROFILE AND OBSERVED BLACK INDICATOR 782

◈ IN PROFILE AND NOT OBSERVED CROSS INDICATOR 784

◇ NOT IN PROFILE OPEN INDICATOR 786

FIG. 7

ARTICLE SUBMITTED

HARDWARE ARCHITECTURE

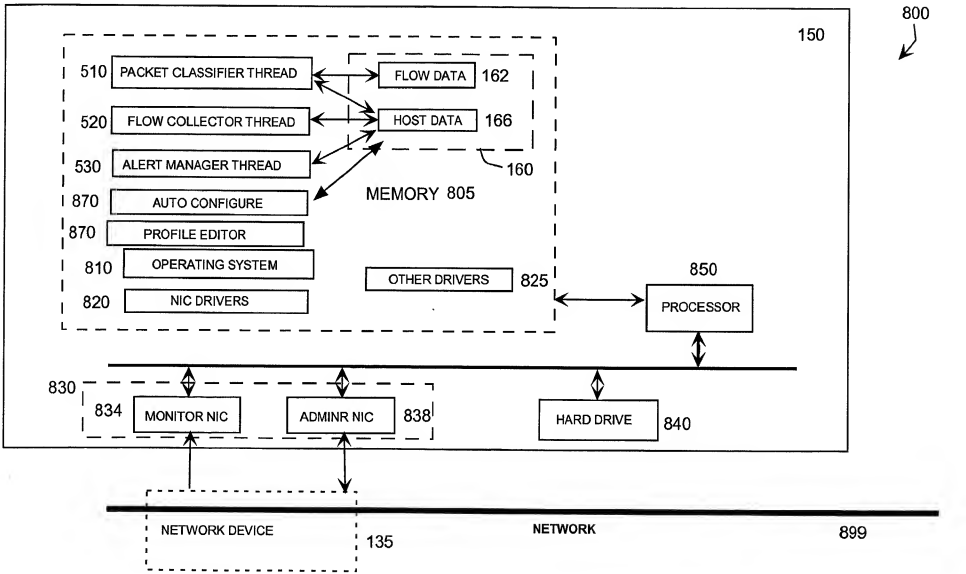


FIG. 8

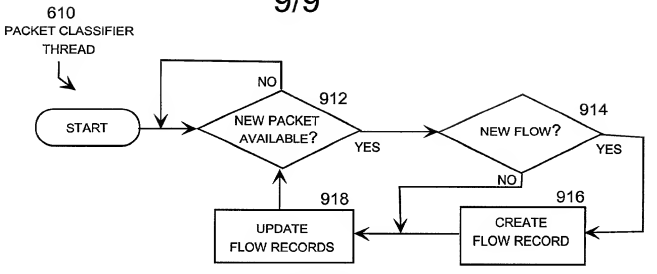


FIG. 9A

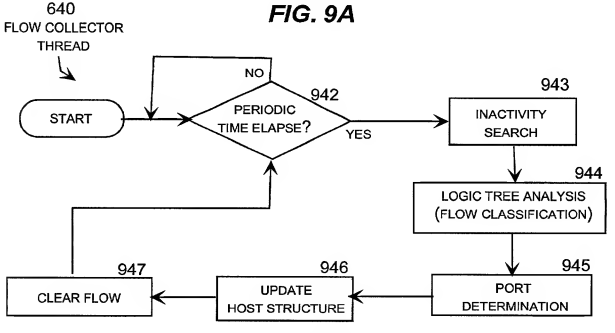


FIG. 9B

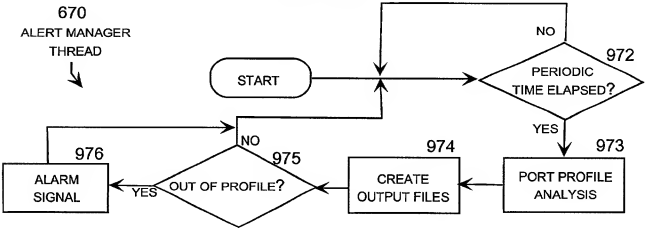


FIG. 9C